Title (en)
Security policy enforcement systems

Title (de)
System zur Durchsetzung einer Sicherheitspolitik

Title (fr)
Systèmes permettant l'application d'une politique de sécurité

Publication
EP 1378813 A2 20040107 (EN)

Application
EP 03445083 A 20030630

Priority
SE 0202050 A 20020702

Abstract (en)
Detection policies must be viewed as delicate and valuable assets in a system. Given the knowledge of the detection policy, an intruder would potentially know how to penetrate the target systems and how to circumvent a Security Policy Enforcement System to avoid detection of his actions. The policies need to be protected from reverse engineering in order to be useful in the context of secure policies (i.e. to prevent disclosure of the detection policy). This invention address the problem of protecting the detection policy in a Security Policy Enforcement System against disclosure to unauthorized persons. The invention protects a detection policy by utilising an irreversible transform function, such as an one-way function or a public/secret encryption scheme, to transform the states of a Security Policy Enforcement System finite-state machine. The Security Policy Enforcement System executes/operates these transformed states and state transitions, which means that it is impossible to study its function by use of so called reverse engineering. The input data to the Security Policy Enforcement System will control the execution path of state transitions to an end-state/access-state. In the end-state, the Security Policy Enforcement System will generate a response, if the detection policy have been violated or not. The invention relates to a security device, to a method for creating a Security Policy Enforcement System performing classification of input events in accordance with a predefined rule-base of detection policy elements, to a method for intrusion detection in a computer and information system having a Security Policy Enforcement System and to computer program products for implementing said methods. <IMAGE>

IPC 1-7
G06F 1/00

IPC 8 full level
G06F 21/55 (2013.01)

CPC (source: EP)
G06F 21/55 (2013.01)

Cited by
US2017034128A1; CN100456692C; CN107092833A; CN100452037C; US10701036B2; US7987496B2; WO2015053906A1; WO2007072157A3; WO2005071923A1; US9477835B2; US8042151B2; US8458770B2

Designated contracting state (EPC)
AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HU IE IT LI LU MC NL PT RO SE SI SK TR

DOCDB simple family (publication)
EP 1378813 A2 20040107; **EP 1378813 A3 20050914**; **EP 1378813 B1 20080213**; AT E386291 T1 20080315; DE 60319034 D1 20080327; EE 200300261 A 20040216; NO 20032873 D0 20030623; NO 20032873 L 20040105; SE 0202050 D0 20020702; SE 0202050 L 20040103; SE 523140 C2 20040330

DOCDB simple family (application)
EP 03445083 A 20030630; AT 03445083 T 20030630; DE 60319034 T 20030630; EE P200300261 A 20030701; NO 20032873 A 20030623; SE 0202050 A 20020702